(12) UK Patent Application (19) GB (11) 2 376 332 (13) A

(43) Date of A Publication 11.12.2002

(21) Application No 0106663.8

(22) Date of Filing 16.03.2001

(71) Applicant(s)
Consignia Plc.
(Incorporated in the United Kingdom)
148 Old Street, LONDON, EC1V 9HQ,
United Kingdom

(72) Inventor(s)
Asha Patel-Evans
David Paul Coward
Peter John Alistair Catherwood

(74) Agent and/or Address for Service
R.G.C.Jenkins & Co
26 Caxton Street, LONDON, SW1H ORJ,
United Kingdom

(51) INT CL[7]
G06K 5/00

(52) UK CL (Edition T)
G4M MB4 MCA
U1S S2268

(56) Documents Cited
WO 2002/050765 A1 WO 2000/031692 A1
US 6039257 A US 5929415 A
US 5917925 A US 5801364 A

(58) Field of Search
UK CL (Edition T) G4M MCA
INT CL[7] G06K 5/00 7/00 7/10 7/12 7/14 17/00
Other: Online:WPI, EPODOC, JAPIO

(54) Abstract Title
Authenticating postage marks

(57) A method of authenticating a postage mark includes the steps of:
extracting an item of information from one component of the mark 152,
extracting a corresponding item of information from a database 158;
comparing the items of information extracted from the postage mark and the database 156, and
determining the validity of the postage mark on the basis of said comparison. For example the postage mark may be declared invalid if a unique number encoded therein is stored in the database 156 indicating that it has previously been used.

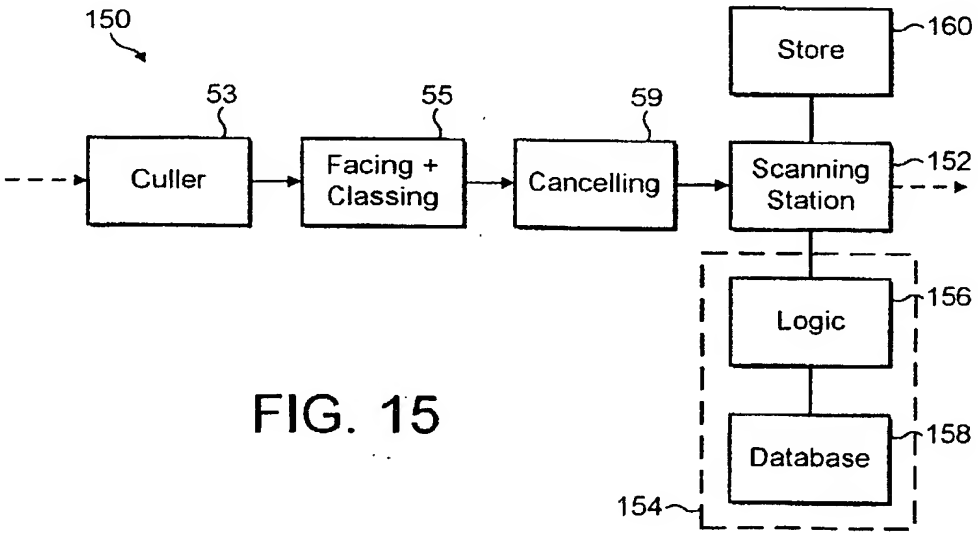

FIG. 15

GB 2 376 332 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

The print reflects an assignment of the application under the provisions of Section 30 of the Patents Act 1977.

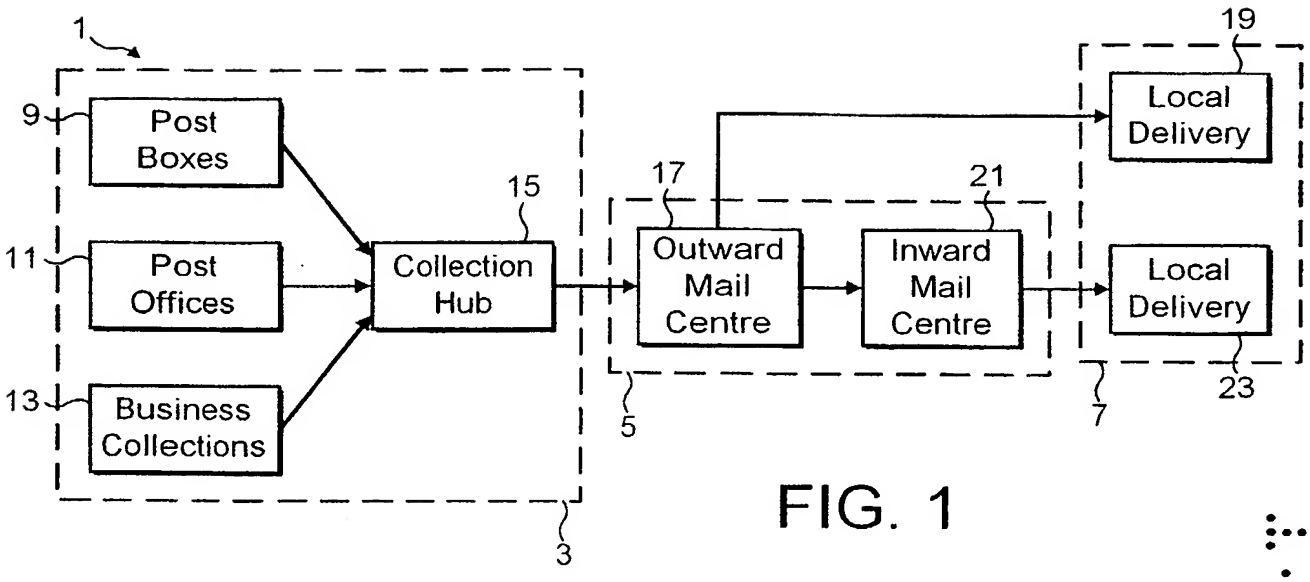

FIG. 1

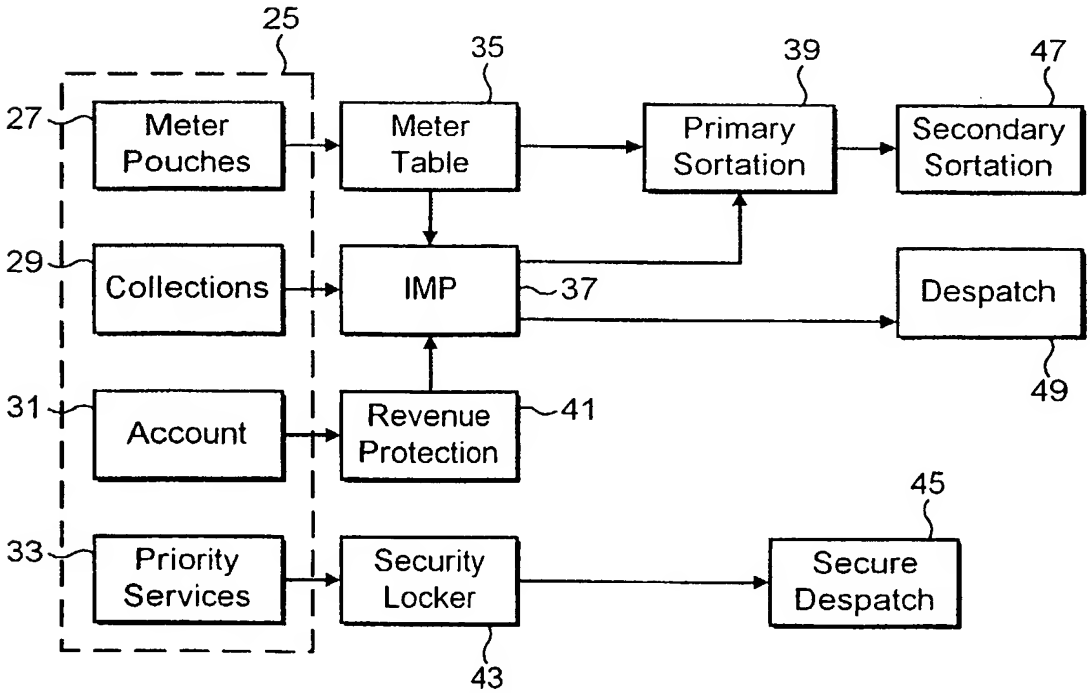

FIG. 2

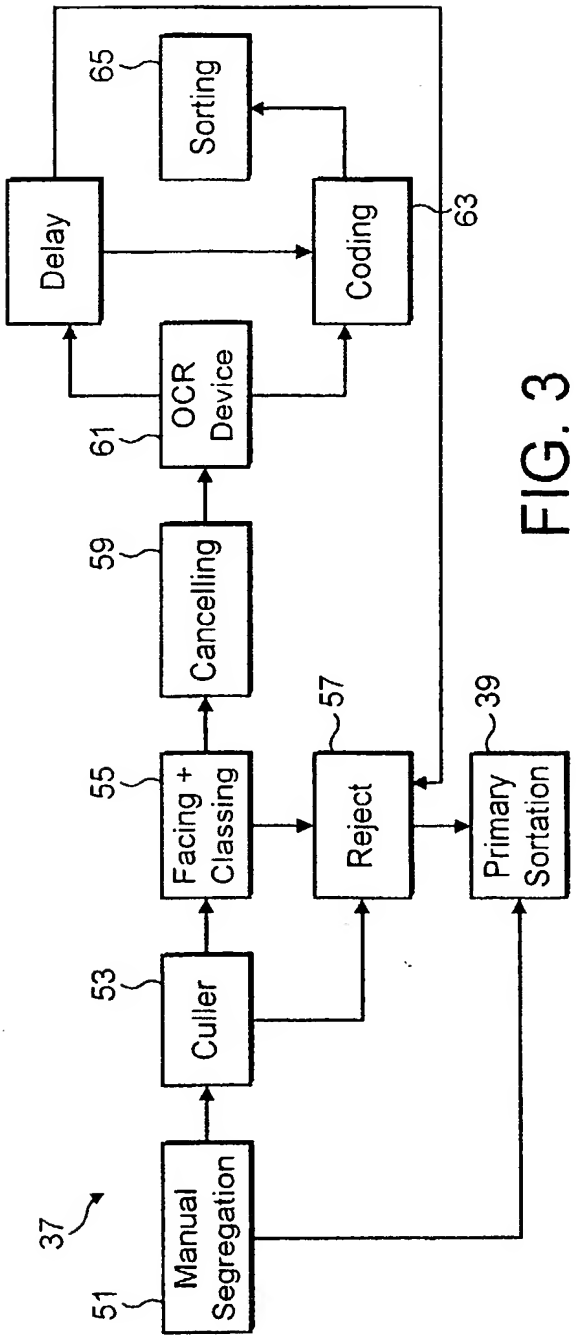

FIG. 3

FIG. 4 67

Symbol	Code
0	--++ / --++
1	-+-+ / --++
2	-++- / --++
3	+--+ / --++
4	+-+- / --++
5	++-- / --++
6	--++ / -+-+
7	-+-+ / -+-+
8	-++- / -+-+
9	+--+ / -+-+
A	+-+- / -+-+
B	++-- / -+-+
C	--++ / -++-
D	-+-+ / -++-
E	-++- / -++-
F	+--+ / -++-
G	+-+- / -++-
H	++-- / -++-
I	--++ / +--+
J	-+-+ / +--+
K	-++- / +--+
L	+--+ / +--+
M	+-+- / +--+
N	++-- / +--+
O	--++ / +-+-
P	-+-+ / +-+-
Q	-++- / +-+-
R	+--+ / +-+-
S	+-+- / +-+-
T	++-- / +-+-
U	--++ / ++--
V	-+-+ / ++--
W	-++- / ++--
X	+--+ / ++--
Y	+-+- / ++--
Z	++-- / ++--

FIG. 5

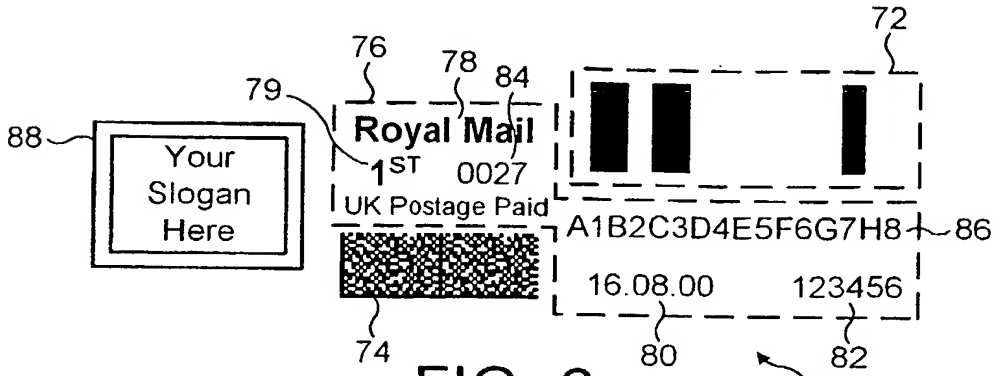

FIG. 6

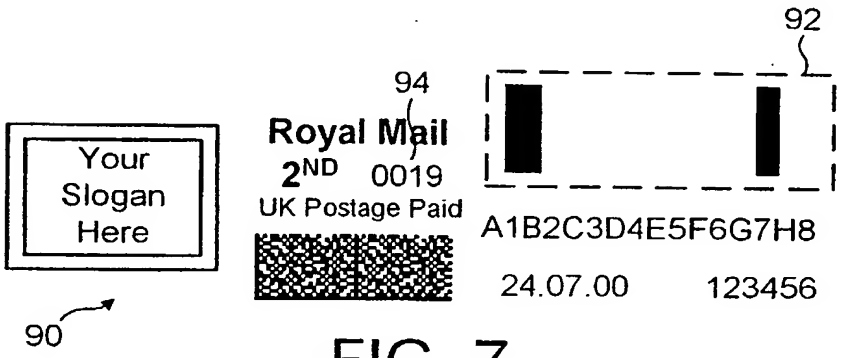

FIG. 7

FIG. 8

FIG. 9

Message	Data Constructs	Data Elements	Format Data	Message Data	Bit Count	Full Bytes
			Message Header	D>^{R}S		1
			FACT Format Header	06^{G}S	c	
			Fact Prefix	J		1
		Licensing Post Identifier		GBA		3
		Account reference		an*6		6
		device reference		a*4		4
Digital Post Mark		batch number or licence number		n*6		6
Main Message		Item number		n*6		6
		Data Format identifer		n*1		1
		Postcode		an*9		9
		Service code		an*4		4
		Postage Value		n*4		4
		Data		n*4		4
		key version		an*2		2
		MAC1, MAC2, Digital signature			54	7
			FACT Format Trailer	^{R}S	c	
			Message Trailer	^{E}O$_{T}$	c	

FIG. 10

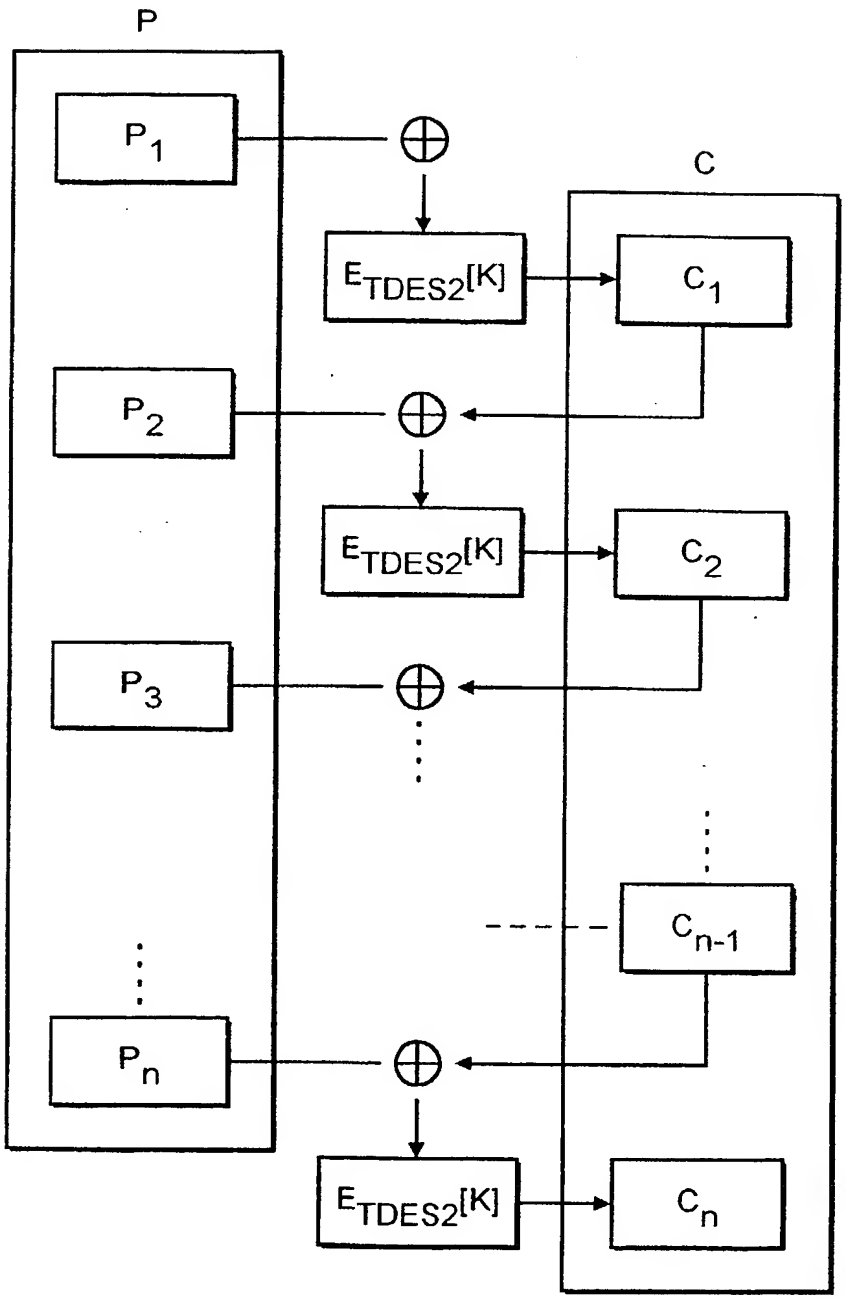

FIG. 11

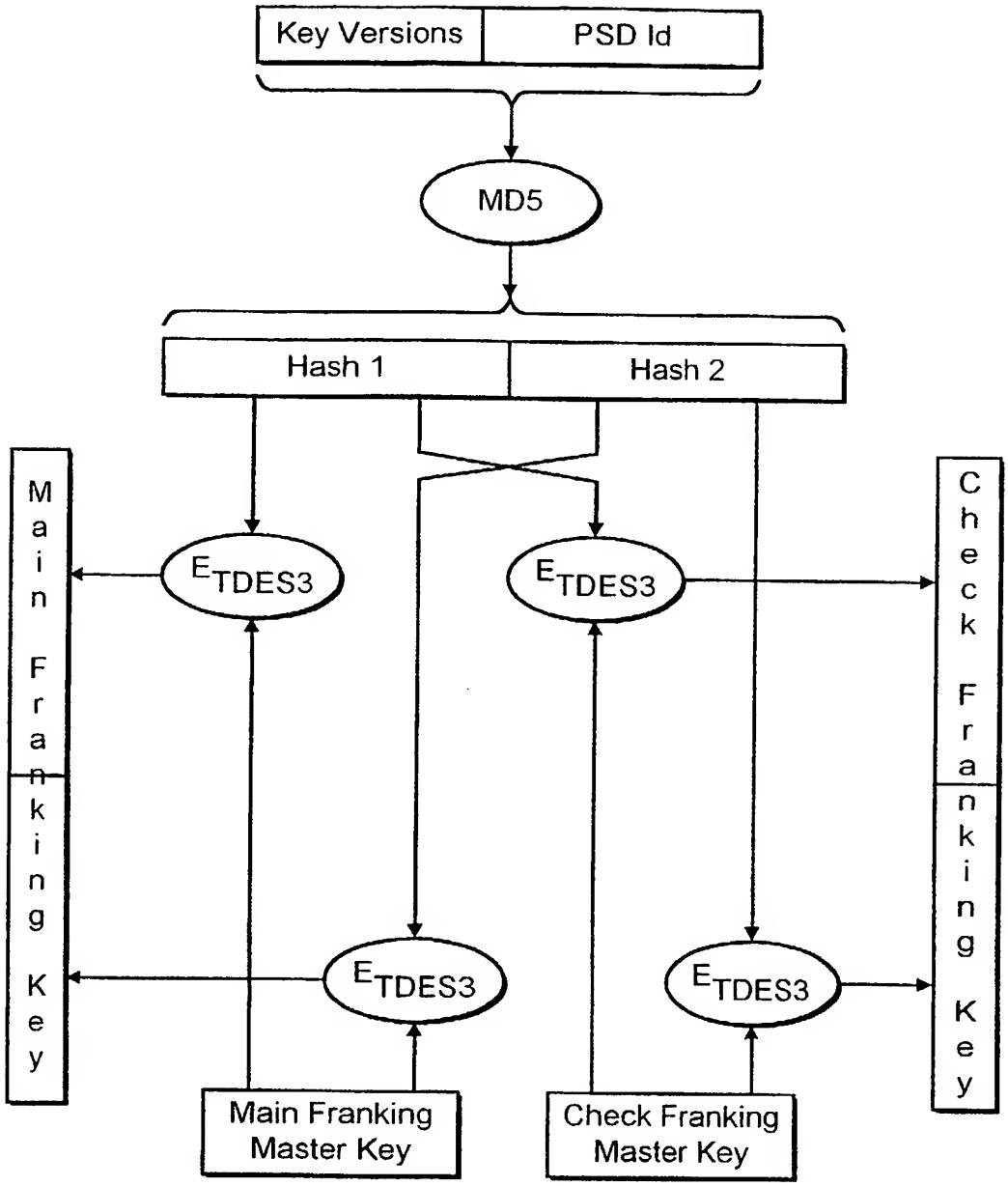

FIG. 12

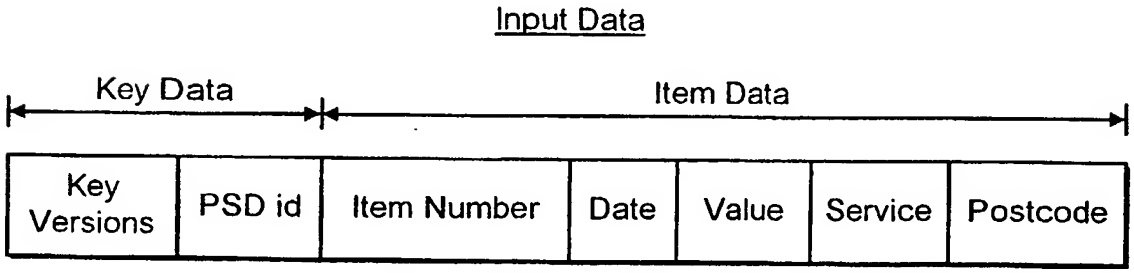

FIG. 13

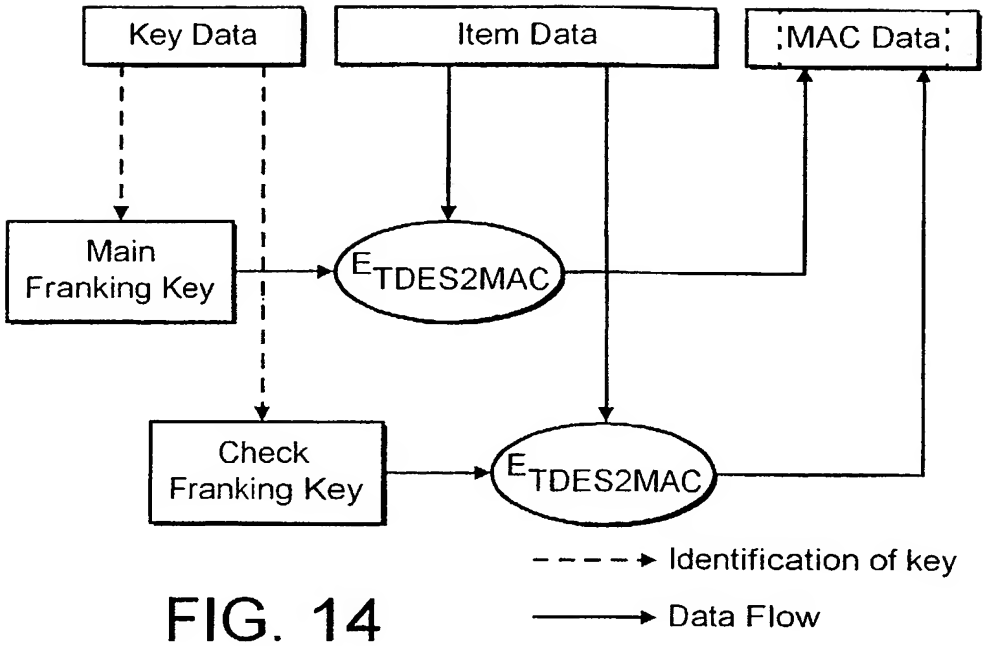

FIG. 14

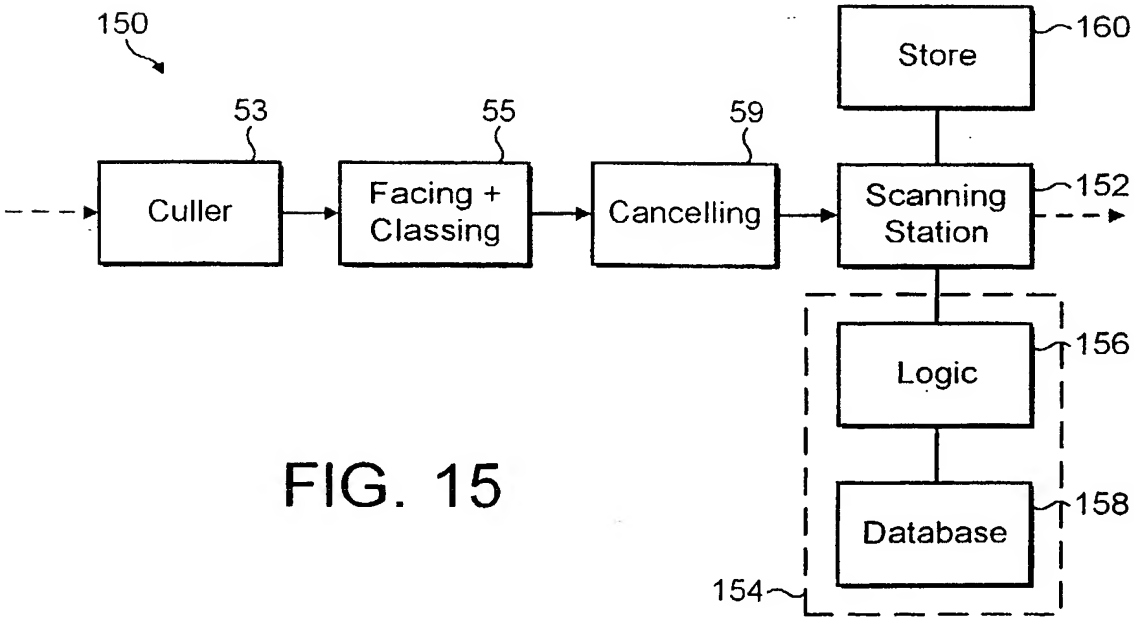

FIG. 15

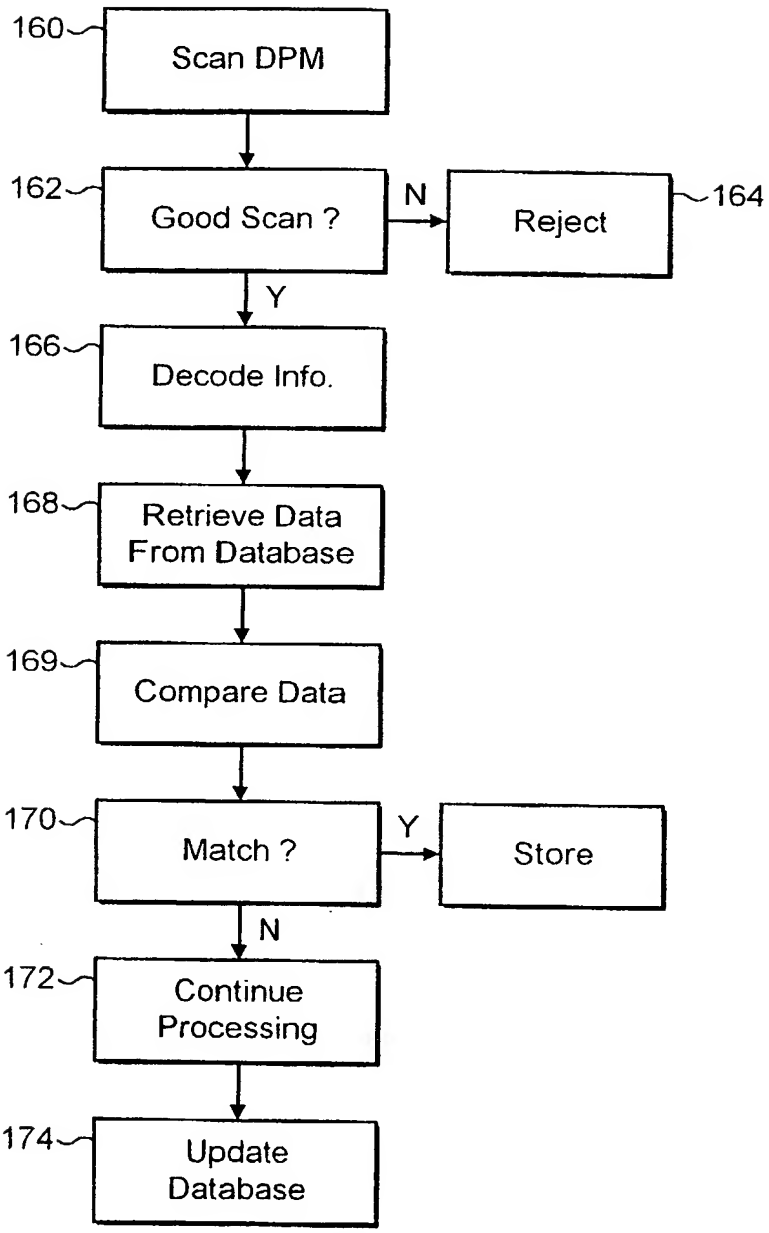

FIG. 16

IMPROVEMENTS RELATING TO POSTAL SYSTEMS

This invention relates, in general terms, to improvements in Postal Systems, and in particular to the use of Digital Postage Marks (DPMs) in such systems.

Before embarking upon this description, it is worth noting at this juncture that Digital Postage Marks (or postage paid indicia as they will also be referred to) should not be confused with conventional postmarks which are used to indicate that postage applied to postal items has been cancelled. Digital Postage Marks are indicia applied to postal items which indicate the postage paid (amongst other things), whereas conventional postmarks are applied after postage has been purchased to cancel that postage.

Figure 1 is a schematic illustration of the various components of a known postal system, such as that which has been operated successfully for many years by the Royal Mail on behalf of the United Kingdom postal authorities.

As shown in Figure 1, collection and delivery of postal items (such as letters, postcards, parcels etc.) in the Postal System 1 is split into three general stages, a collection stage 3, a sorting stage 5, and a delivery stage 7.

At the collection stage 3 postal items are collected from a variety of different sources, such as from post boxes 9 dotted around the country, from post offices 11 where the postal items have been handed by the public to the postal authorities, and direct from businesses 13.

The collected postal items are gathered together at local nodes of the postal system and are then sent to one or more district collection hubs 15 where postal items from a number of local nodes are gathered together.

In the second stage 5 of the postal system, all the items sent to the district collection hubs 15 are sent to a so-called "outward" mail centre 17 for sorting. The outward mail centre 17 is so named because it deals with postal items that are on their way out of the postal system to the addressee of the item.

At the outward mail centre 17, incoming postal items from the collection hubs are sorted into those items which are destined for delivery in designated districts surrounding the outward mail centre (local items), and those which are destined for delivery to other districts which are further afield (remote items).

Local items are finely sorted (for example into items for particular towns and/or streets) and are then sent on from the outward mail centre to appropriate local delivery offices 19 for delivery to the postal item addressees in the third stage 7 of the postal system 1.

Remote items are roughly sorted (for example into items for particular regions of the country) and are sent onto the appropriate inward mail centre 21 for each region of the country. At the inward mail centre (so named because it deals with postal items that are coming into the postal system prior to delivery) the items received from the outward mail centre 17, and from

elsewhere, are finely sorted into, for example, items for particular towns and/or streets.

The third and final stage of the postal system 1 is the delivery stage 7 where postal items sorted by the inward mail centre 21 are transferred to local delivery offices 23 for delivery to the postal item addressees. At this stage of the process the local items sorted by the outward mail centre 17 are also delivered by the local delivery offices to the item addressees.

Figure 2 is a schematic illustration of the various processes which occur when postal items are sorted at one of the aforementioned mail centres for example the outward mail centre 17.

As shown in Figure 2, postal items of a variety of different types arrive at the mail centre from the collection hub 15. The arriving postal items 25 can be roughly split into those items 27 (meter pouches) which have been presorted into class pouches (red pouches for first class mail, green pouches for second class mail) by customers, those items 29 which have been collected from post boxes 9 and post offices 11, those items 31 which have been received from customers with Royal Mail accounts, and those priority service items 33 which have an additional payment for one of the many different types of priority service.

Typically, presorted items in meter pouches 27 are those which have been collected from businesses in the collection stage 3 of the postal system shown in Figure 1. Account items are typically from businesses which send

out a large amount of correspondence, for example direct mailing companies. Account items are often known as PPI mail (or Printed Postage Impression mail) due to the fact that the envelopes used are usually preprinted with the appropriate postage. Collection items 29 will typically not have been sorted for class of service (e.g. 1st class or 2nd class), or for size of mail.

In the next stage of the sorting process, postal items in meter pouches 27 are transferred to a meter table 35 where the postal items are manually removed from the pouches and either transferred to an Integrated Mail Processor 37 (known as an IMP) or direct to a primary sortation facility 39 for further processing.

Collection postal items 29 once received by the mail centre 17 are transferred to the IMP 37 for further processing. Account postal items 31 are passed first to a revenue protection facility 41 before also being passed to the IMP 37.

In the revenue protection facility 41, bags of postal items received from account customers are weighed, and the read weight is checked against a bag weight printed by the customer on a ticket attached to the bag. The charge billed to the customer's account can be adjusted in the event of any discrepancy between the weight declared by the customer and the weight read by the revenue protection facility.

Priority service postal items 33 are kept separate from the remainder of the postal items and are passed to a security locker 43 where they are sorted

prior to being dispatched at a security despatch station 45.

As mentioned above, all of the collection items 29, some or all of the meter pouch items 29, and the account items 31 are passed to the IMP 37 for sorting. Any mail unsuitable for sorting via the IMP 37 is rejected and sent to the primary sortation facility 39.

The operation of the IMP will later be described, but at this juncture it suffices to mention that the IMP operates (for those items which can be automatically sorted):

(i) to detect the class of the postal items (i.e. whether first or second class);

(ii) to cancel postage applied to the postal items;

(iii) to apply a machine readable code which identifies both the class and the destination to the postal items, and

(iv) to sort the postal items by destination.

Any items which cannot be processed by the IMP 37 (or meter pouch items 27 not routed via the IMP), for example because they have an unusual shape or because the address cannot be read, are passed to the primary sortation facility 39 where they are fine sorted by hand into mail for local regions and rough sorted into mail for remote regions. The items for the remote regions are then passed to a secondary sortation facility 47 where they are more finely sorted.

Once the postal items have been sorted; either by the IMP 37 or by the

primary and secondary sortation facilities 39, 47; they are passed to a despatch facility 49 where they are despatched to local delivery facilities or to an inward mail centre 21 such as that described above with reference to Figure 1.

Figure 3 provides an illustrative schematic view of the various components of the IMP 37.

In a first step 51, the IMP 37 is manually loaded with postal items with obviously outsize (or otherwise objectionable) postal items being rejected by the individuals loading the machine.

The postal items entering the IMP pass up a conveyor belt to a culler 53 where the postal items are spun in a rotating drum. The sides of the drum are slotted so that postal items which are suitable for automatic processing fall through the slots. Postal items which are too large for automatic processing are rejected (in step 57), and move through the drum and fall out the end. These outsize, or otherwise unsuitable, items are collected and taken to the primary sortation facility 39 for hand sorting. Typically, the IMP will reject any postal items which have a thickness that is greater than 6mm or so.

Postal items falling through the slots in the drum in the culler 53 are passed to a facing an classing unit 55 where the items are appropriately orientated, and the postal class of the items is determined. Again, any items which cannot be classed, or which cannot be faced are rejected (in step 57) and passed to the primary sortation facility 39 for hand sorting.

Correctly faced and classed postal items are then passed to a

cancelling unit 59 which cancels postage applied to the items by overprinting the postage with a post mark. Once the postage has been cancelled the items are passed to an OCR device 61 where an image is taken of the address block on the item and an optical character recognition process is employed to attempt to determine the postal code of the address block.

If the postal code can be determined by the OCR device 61, then a code is applied to the front of the postal item by a coding device in step 63 and the item is sorted in accordance with the applied code in step 65.

If the postal code cannot be read for any of these items, the image of the address block is sent to a remote post code determining suite and the items in question are passed to a delay line 63 which sidelines the postal item in question for a predetermined period of time. Whilst a given item is in the delay line, an operator in the post code determining suite is presented with the image of the address block and that operator is provided with a short period of time to determine and input the correct post code from the image presented. The correct inputted post code, once inputted, is assigned to the associated postal item, and the item is then coded (in step 63) and sorted (in step 65).

If the operator cannot identify the correct post code from the image presented, then the item concerned is rejected (in step 57) and passed to the primary sortation facility 39 for hand sorting.

As shown in Figure 2, items which have been correctly coded and sorted by the IMP 37 are passed directly to the despatch facility 49 where they

are despatched to local delivery facilities or to an inward mail centre 21 such as that described above with reference to Figure 1.

Figure 4a is a schematic illustration of a coded indicia 67 of the type typically applied by the coding unit 63 of the IMP 37 shown in Figure 3.

The coded indicia shown in Figure 4 is a so-called "four state bar code", and is sometimes referred to as the Royal Mail 4-State Customer Code (RM4SCC). The RM4SCC was specially developed by the Royal Mail for automated mail sortation processes, and is used to print the postcode and delivery point suffix (DPS) which identifies both the destination point of the postal item and the identity of the post office from which delivery of the item will be made. Four State Barcodes are also used, amongst others, by the Dutch and Canadian postal authorities.

The RM4SCC is based on 36 barcodes which are capable of representing alphanumeric characters 0 to 9 and A to Z, and start and stop characters "(" and ")" respectively. As shown in Figure 4a, in the barcode a small black bar extends upwards, downwards or in both directions, and any one alphanumeric symbol is encoded by four bars – two of which have an upward extension and two of which have a downward extension.

Figure 4b illustrates in graphical form the bar combinations and corresponding alphanumeric symbols. In Figure 4b, the symbols to the left of the slash represent upward bar extensions and the symbols to the right of the slash represent downward bar extensions. In each case, a plus symbol means

that the bar is extended and a minus symbol means that the bar is not extended.

As has been briefly mentioned above, postage is applied to postal items prior to those items being collected by the postal authorities. In the case of individual customers, that postage is most likely to be in the form of gummed stamps which the customer purchases, for example from a post office, and then affixes to the item or items to be posted.

Corporate customers tend not to use individual gummed stamps since the process of dampening the gummed layer and affixing the stamp to individual items would be very labour intensive if a large number of items were to sent out in any one day. For these customers, the Post Office – amongst others – have developed so called Franking Machines which can be operated to print postage paid indicia onto self-adhesive labels which can then be affixed to the item or items to be posted.

Franking machines (such as the FRAMA® Sensonic 2100 manufactured by FRAMA AG of Lauperswil, Switzerland) are preloaded with postal credit purchased by a customer from the Post Office or one of their agents. To use the franking machine the customer must first weigh the postal item and select the class of postage required. The price for that postal weight and postal class is then displayed and the price must then be entered into the franking machine. The customer then inserts one of the aforementioned self adhesive labels into the machine and a postage paid indicia is printed onto the

label to indicate that postage amounting to the price indicated has been paid. At the same time, the postal credit stored on the franking machine is debited by the amount of postage printed onto the label. Postal credit on the franking machine can be topped up, upon payment, as required by the customer, and is stored in a secure Postal Security Device (PSD) of the franking machine. The PSD functions to account for value credits to the franking machine and postal debits therefrom.

Typically, the meter pouch postal items 27 referred to above in Figure 1 will be franked postal items that each bear one of these postage paid self-adhesive labels.

In addition to stamped mail, and franked mail, there are also other mechanisms for prepaying postage. For example, it is commonplace for companies to send out business reply envelopes which are pre-printed with postage paid indicia. It is also commonplace for companies who are sending large amounts of mail (the companies referred to in Figure 1 as account customers sending account mail 31) to use envelopes that have been pre-printed with postage paid indicia.

This system, whilst it has functioned adequately for many years, does have a number of associated problems.

As will be immediately apparent from Figure 2, it is only the account mail (from, for example, bulk customers of the post office) which is submitted to the revenue protection facility 41.

Franked mail (which will typically arrive within the meter pouches 27 shown in Figure 1) is provided with a cursory check at the collection hub 15 before it is transferred to the outward mail centre 17, but it is not reviewed by the revenue protection facility.

It has recently come to the attention of the Post Office that the checks performed on this franked mail are not satisfactory as there are many ways of reproducing postage paid indicia on self-adhesive labels without an associated debit of the postage credit stored on the franking machine.

Even if each and every item of franked mail were to be subjected to an individual inspection, items of mail with fraudulent postage paid indicia would still get into the postal system as it is not always possible to spot a fraudulent indicia by visual inspection.

Obviously, for security reasons it is not appropriate to explain in this document how these fraudulent indicia can be produced. It will suffice for the purposes of the present document to state that this is a serious problem, and that the Post Office are potentially losing a significant amount of income from fraudulent activity of this type.

Another problem associated with the use of franking machines is that companies are typically required to hire the franking machine from the Post Office or their agents. The hire of these machines can be quite a significant expense especially for small companies who do not produce large quantities of mail, but nevertheless do not want to have to use gummed stamps.

A further problem is that the franking machines are typically preloaded with a not inconsequential sum of money, which the company concerned cannot use once it has been used to charge the machine.

To alleviate some of these problems it has been proposed to provide so-called PC franking, where postage paid indicia can be printed onto envelopes using one of a number of normal desktop printers connected to a standard computer, such as a PC for example. Pitney Bowes and a company called Stamps.Com both offer internet based PC Franking systems (see www.stamps.com and www.clickstamp.pb.com for details) where postage can be bought via the internet, and postage paid indicia can be printed onto envelopes using commonly available desktop computers and printers.

These internet systems would seem, at first sight, to resolve most of the problems experienced by small companies as they obviate the need for those companies to hire franking machines and precharge them with credit.

However, PC based systems only make the Post Office's revenue protection processes even more problematic as someone using such an internet system is provided at his desk with a computerised postage paid indicia which could, potentially, be manipulated and fraudulently used.

It is an object of the present invention to avoid, or at least alleviate, the problems outlined above, and in particular to provide a digital postage mark (for use with franking machines, with PC franking or a printed postage impression, for example) that assists in the alleviation of these problems.

In pursuance of this object, various aspects of the present invention are defined in the accompanying claims. Particular embodiments of those aspects, which are currently preferred, are set out in the accompanying dependent claims.

It should be noted, however, whilst particular features have been selected as being of interest, the invention is not so limited and can comprise any combination or permutation of features set out herein whether or not that combination or permutation has explicitly been claimed.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic illustration of the various components of a known postal system;

Figure 2 is a schematic illustration of the various processes which occur when postal items are sorted at one of the outward mail centres shown in Figure 1;

Figure 3 is a schematic illustration of the various components of an IMP such as that shown in Figure 2.

Figure 4 is a schematic illustration of a coded indicia of the type typically applied by the IMP shown in Figure 3;

Figure 5 illustrates, in graphical form, the bar combinations and corresponding alphanumeric symbols of the coded indicia shown in Figure 4;

Figure 6 is a schematic representation of a digital postage mark;

Figure 7 is a schematic representation of another digital postage mark;

Figure 8 is a schematic representation of another digital postage mark;

Figure 9 is a schematic representation of another digital postage mark;

Figure 10 is a schematic representation of a message encoded within a data matrix;

Figure 11 illustrates use of a CBC mode in an encryption function;

Figure 12 illustrates a process for generating a main franking key, and a check franking key;

Figure 13 is a schematic representation of data elements used for constructing an integrity hash, a main MAC and a check MAC;

Figure 14 is a schematic representation of a MAC generation process;

Figure 15 is a schematic representation of part of an integrated mail processor; and

Figure 16 is a flow diagram illustrating steps of a revenue protection process.

Before embarking upon a description of the preferred embodiments, it is useful to point out that the teachings of the present invention are equally applicable to digital postage marks printed onto envelopes using the aforementioned PC franking process, digital postage marks printed onto self-adhesive labels in franking machines, and so-called PPI mail. Accordingly, whilst the description provided below will tend to concentrate on postage marks printed in a PC franking process (such as those described above) it

should be noted that the invention can be used in other systems, and the scope of the invention should not be read as being limited to PC franking by the description provided.

Figure 6 is a schematic representation of a first digital postage mark 70. As shown, the postage mark 70 is composed of a number of constituent parts, and it should be noted that not all of these constituent parts are essential to the present invention.

The postage mark 70 comprises, in this arrangement, a so-called facing identification mark 72 (referred to in the art as a FIM) which serves two purposes. FIMs are commonly used in business reply mail to indicate to automated mail sorters (such as the IMP 37 described above), the class of postage that has been paid for.

In the arrangement of Figure 6, the FIM comprises two broad marks next to one another, and a further broad mark separated from the other two marks. This combination of marks indicates to the automated mail sorter that the postage paid is sufficient for 1st Class mail.

In addition to indicating the class of postage paid, the FIM also functions to provide automated mail sorters (such as the IMP 37 of Figure 1) with a means to easily locate the face of the envelope on which the address is likely to be written or printed.

In addition to the FIM (which as will later be described need not be provided) the postage mark 70 comprises a data matrix 74 within which

information is encoded. The information encoded, and the encoding mechanism will later be described. It is preferred that the data matrix is a particular type of two-dimensional matrix, but it will be appreciated that other types of data matrices may be employed if desired. For example, the data matrix could comprise a Maxicode 2D matrix, further details of which may be found at: www.maxicode.com.

The postage mark 70 also includes various items of text which can be read by a human, or by an OCR device in an automated mail sorter. For convenience these text items will be referred to herein as "user readable text" 76, and it should be noted that the "user" can be a human or a machine.

The user readable text 76 comprises:

(1) standard text 78 which does not change and is always printed (in this case the text "Royal Mail", and "UK Postage Paid"),

(2) a class indication 79 (in this case "1st") which varies in accordance with the class of postage paid for (and which is indicated in this arrangement by the FIM),

(3) a date mark 80 (in this case "16.08.00") which indicates the date on which the postage mark was printed,

(4) an item number 82 (in this case "123456") which indicates the item number assigned to the postage mark,

(5) a value mark 84 (in this case "0027" – representing 27 pence postage paid) which indicates the amount of postage paid, and

(6) an encrypted mark 86 (represented in the figure as "A1B2C3D4E5F6G7H8") which is readable by the user but which does not provide any useful information until it has been decrypted. As the encrypted mark is readable, but not intelligible by a user, it can be manually entered into revenue protection devices (to be described) in the event that the data matrix should be unreadable.

In addition to these marks, the postage mark 70 may optionally include a space 88 for a user to print a slogan or company logo.

As mentioned above, in the preferred arrangement information (some of which is encrypted) is encoded to generate the data matrix, and information is encrypted to generate the encrypted mark. In an alternative arrangement, which is not presently preferred, more of the information for generation of the data matrix may first be encrypted before being encoded to generate the data matrix.

Figure 7 is a schematic representation of a second digital postage mark 90. The second mark whilst being similar to the first mark in a number of respects, differs principally in that the FIM 92 in this arrangement is different to that of the first arrangement.

As shown in Figure 7, the FIM 92 comprises a pair of broad marks which are spaced from one another and this configuration indicates to automated mail sorters that the postage paid is sufficient for 2nd Class mail.

As the class of postage is different in the second mark, the value mark

94 (in this case "0019" – representing 19 pence postage paid) is different to that of the first mark.

In addition, as the class of postage has changed the data matrix 96 and also the encoded text 98 will be constructed (as will later be described) from different information (notwithstanding the fact that other items of information encoded in these marks will also change). The differences between the encoded text and data matrix of the first and second marks need not necessarily be apparent upon a visual inspection of the marks, as the marks may need to be decoded before the differences are apparent.

Figures 8 and 9 show third and fourth marks that differ from the above described first and second marks in that the postage mark does not include any FIMs. As is mentioned above, FIM do not necessarily need to be provided in order for mail to be sorted by an automated mail sorter.

In all other respects the marks shown in Figures 8 and 9 are identical to those of Figures 6 and 7.

At this juncture, and before embarking upon a description of particular features of this invention, it is useful to describe the preferred form of data matrix in detail, and also the means by which information is encrypted within the DPM.

The Data Matrix

As mentioned above, this description relates to one particular example of a two dimensional data matrix, and it will be appreciated by persons skilled in the art that alternative data matrices may be employed without departing from the scope of the invention. Accordingly, the present description should not be read as limiting the scope of this invention.

A number of standards currently exist for two dimensional data matrices, and reference may be made to the following standards in the forthcoming description where it is appropriate to do so:

- UPU Standard S21-1: Data Presentation in ASN.1
- UPU Standard S24-1: FACT-Based Representation of Postal Information and Identifiers
- UPU Standard S25-1: Data constructs for the communication of information about postal items, batches and receptacles
- UPU Standard S27-1: Framework for communication of information about postal items, batches, and receptacles
- UPU Standard S28-1: Communication of postal information using two-dimensional symbols
- ISO 04217: Specification for codes for the representation of Currencies & Funds
- ISO DIS 15394: Bar Code and Two Dimensional Symbols for

Shipping, Transport and Receiving Labels

- ISO 15418: Automatic Identification and Data Capture Techniques – International Specification – Data Application Identifiers
- ISO 15434: Transfer Data Syntax for High Capacity ADC Media
- International Symbology Specification – Data Matrix, published in 11/96 with editorial amendments dated 12/96 (V1.01), and an erratum dated 23/7/97.

It has been mentioned above that the Data Matrix of the digital postage mark contains encoded information. This encoded information will generally be referred to as a "Message" containing a number of "Data Elements" each relating to a different item of information.

A complete DPM message may be encoded in one two dimensional symbol, or optionally in more than one (for example, two) two dimensional symbols.

Each DPM message comprises: a Message Header, a number of data elements, and a Message Trailer.

The Message Header consists of two parts, a *Compliance Indicator* and a *Format Trailer Character*. In this system, the Compliance indicator comprises three characters [)>, and the *Format Trailer Character* comprises the 8 bit hexadecimal value 1E (ASCII $^{R}_{S}$)].

The data elements mentioned above are encoded in a block comprising:

(1) a *Format Header*, comprising a Format Indicator (in this case value 06 for FACT Data Constructs) followed by a Data Element Separator (in this case hexadecimal value 1D (ASCII $^{G}_{S}$));

(2) the data elements; and

(3) a *Format Trailer character* (in this case $^{R}_{S}$).

The *Message Trailer* comprises the 8 bit hexadecimal value 04 (ASCII$^{E}o_{T}$).

In summary, each message comprises: a Message Header, a Format Header, Data Elements, a Format Trailer and a Message Trailer. This message structure is shown diagrammatically in Figure 10.

Additional customer defined message(s) may be agreed with a customer, and these messages will be included in one or more further data matrices (not shown).

The Data Elements of the message described above may comprise information concerning one or more of the following:

(1) a FACT Prefix;

(2) a licensing Post Identifier;

(3) an account reference;

(4) a device reference;

(5) a batch number or licence number;

(6) an item number;

(7) a data format identifier;

(8) item data or a postcode (including delivery point information);

(9) a service code;

(10) a postage value;

(11) a date;

(12) a key version;

(13) one or more message authentication codes (MACs), and

(14) a digital signature.

The FACT prefix in this case is defined as ASCII J, and is provided to indicate that the data following the prefix is issued under an authority granted by the Universal Postal Union (UPU).

The Licensing Post Identifier data element is a three ASCII character field identifying which postal administration has authorised a given customer to encode messages in accordance with the mechanism described herein. In the United Kingdom, the Licensing Post Identifier would be GBA for the Royal Mail.

The Account Reference data element is a field of six alphanumeric ASCII characters. Alphanumeric characters are defined in the context of this document as being upper case alphabetic characters or numeric characters.

The Account Reference, combined with the batch number/licence number and the data format identifier uniquely identifies the licensed entity from whom the mail has originated.

The Device Reference data element is a field of four alphanumeric

ASCII characters formed by a provider identifier (e.g. an identifier for the provider of the franking machine) and a device model number (i.e. the model number of the device by means of which the DPM was printed), each of two characters.

The Batch Number/Licence number data element is defined as a field of six alphanumeric ASCII characters. Each postal item forms part of a batch of mail that is identified through a unique batch number. A batch is defined as either: all of the franked mail items associated with one Statement Of Mailing Submission (in this case the batch number will effectively be the SOMS number); or all of the mail items, whose postage was accounted for by a defined postal security device, franked between two consecutive occasions on which the device was re-credited. Postal Security Devices (PSDs) are secure hardware devices which perform a postal accounting function. PSDs can form part of a franking machine (as mentioned above), or alternatively they may take the form of a PC interface card or a secure device with an interface to a PC such as a smart card, for example.

Batch Numbers begin at '0' and are incremented in steps of one. The Licence number is also known as the customer Account Reference. The data format identifier determines whether this data element describes the batch or the licence, is determined by the data format identifier.

The Item Number data element is defined as a field of six numeric ASCII characters, and functions to identify an individual postal item within a

batch of postal items. Item Numbers begin at '0' and increment in steps of one.

The Data Format Identifier data element comprises one numeral, and is used to identify the type of device or product printing the digital postage mark, i.e. whether the DPM has been produced by PC franking, by a franking machine or is a PPI.

The Item Data / Post Code data element is an application dependent alphanumeric data field. This field is preferably defined by the individual item's Post Code, and comprises up to nine ASCII characters, the first being an alpha, the rest being alphanumeric. The field must be padded with spaces to nine characters in the event that the post code or other data is less than nine characters. If the field contains a Post Code it may be divided into 3 fixed length sub-fields, Outward (four alphanumeric characters), Inward (three alphanumeric characters), DPS (two alphanumeric characters); and all sub-fields are left-justified space padded.

The intention is that this field supports the security and efficiency of the postal system by improving address interpretation and reducing the potential for fraudulent indicia, for example. The preference is that this field contains the item's Post Code, which is a coded representation of the geographic delivery location within the United Kingdom. Space is provided for the outward, inward, and delivery point codes as defined above. If no Post Code is available then up to the first nine characters of the bottom line of the

address may be used (the first must be an alpha), otherwise the field may be filled with all space characters. Depending upon the postal application, the field may contain other alphanumeric data which identifies the item or authenticates the DPM e.g. a serial number for the substrate on which the DPM is printed.

The Key Version data element is defined by two ASCII characters, and is used to identify a set of keys held within a given Postal Security Device.

The Message Authentication Codes (MACs) and Digital Signature data elements are defined by two twenty bit strings, and a fourteen bit string. The MACs and digital signature are used to ensure the authentication and integrity of variable data contained within the message using symmetric encryption for the MACs, and an SHA-1 message digest function (as defined in FIPS180-1; Secure Hash Standard, FIPS Publication 180-1, National Institute of Standards and Technology, May 1993) for the digital signature. Two MACS are used, the main MAC for normal use, and a check MAC for confidence checking. The procedure for encrypting the MACs will later be described in association with the description relating to the encrypted, user readable, mark.

The Service Code data element comprises four alphanumeric characters. In this field, *1CXX* designates first class post service, and *2CXX* designates second class post service. Other postal service classes may later be

defined.

The Postage Value data element is defined by a field of four numeric characters which together define the value of the service provided in UK currency (pence). This is also the postage value accounted for by the PSD when the DPM is generated.

The Date data element comprises a field of four numeric characters which define the month and day on which the DPM is generated in the format "mmdd". A user readable version of this data element is also printed in the DPM, as mentioned above.

As mentioned above, Messages may be represented on mail items and other items by means of two dimensional symbols printed in accordance with the AIM Data Matrix Technical Specification defined in an AIM International Specification entitled International Symbology Specification – Data Matrix, published in 11/96 with editorial amendments dated 12/96 (V1.01), and an erratum dated 23/7/97.

This particular Data Matrix symbology supports a number of variants, of which a variant called ECC200 is one – and it is preferred that this variant of the symbology is used as it uses Reed-Solomon error correction. Any of the compaction modes and Macro Characters supported in the ECC200 variant of the *Data Matrix AIM specification* may be used. Although, it is thought that in practice, only two encodation schemes are likely to be used; ASCII, at the start of the symbol, for encodation of some character data and

for encodation of long numeric strings, and C40 encodation for data streams containing uppercase alphabetic and numeric characters.

The minimum size for a cell of the data matrix in accordance with the preferred arrangement is in the range of 0.60mm for a 300 dpi printer (7 dots) to 0.63mm for a 200 dpi printer (5 dots). A higher cell size may be required depending upon the print resolution. The data matrix symbol is preferably 16 by 48 cells (72 alphanumeric characters) if facing identification marks (FIMS) are required on the mail. Otherwise, a square data matrix of 26 by 26 (64 alphanumeric characters) shall be printed when no FIMS are required.

Whilst the above described AIM symbology supports Extended Channel Interpretation (ECI) it is not proposed to make use of this functionality in the preferred arrangement as there is likely to be little need to encode data from alphabets other than the Latin Alphabet.

As mentioned above, it is possible to provide a number of data matrix symbols adjacent to one another. Preferably a maximum of two data matrix symbols are provided. In any case it is preferred that the Data Matrices include a Quiet Zone of twice "X" between the symbols and between the symbols and other printed data. The first symbol will contain the main franking indicium message while the second, to the left, may contain customer defined data. The Quiet Zone is needed to discriminate the symbol from surrounding printed data. The Data Matrix specification (mentioned above) requires this Quiet Zone to be at least "X" wide on all four sides of the

symbol, but to improve readability on automated postal sorting equipment it is preferred that a quiet zone of a minimum of twice the "X" dimension is provided. The "X" dimension is defined as the intended width of the cells of the data matrix.

Encryption

As mentioned above, the DPM includes an encrypted user readable mark which, whilst being readable by a user, is unintelligible until the mark has been decrypted. The DPM also includes, encoded with the Data Matrix, encrypted MACs and a digital signature.

It will be appreciated by those persons skilled in the art that many different types of encryption exist, and that any of these different types of encryption can be substituted for the particular type of encryption that will now be described, without departing from the scope of the invention.

A number of standards currently exist for data encryption, and reference may be made to the following standards in the forthcoming description where it is appropriate to do so:

- [FIPS46] FIPS PUB 46, "Data Encryption Standard", NIST, January 1977.
- [FIPS81] FIPS PUB 81, "DES Modes of Operation", NIST, December 1980.
- [FIPS180-1] Secure Hash Standard, FIPS Publication 180-1, Nat. Inst. of Standards and Technology, May 93.

- [ISO4217] Currency and Funds Code List.
- [RFC1321] The MD5 Message-Digest Algorithm, R. Rivest, Request for Comments: 1321, April 1992.
- [FIPS 46-3] FIPS PUB 46-3, "Data Encryption Standard", NIST, October 1999.
- [ANSI X9.52] Triple Data Encryption Algorithm modes of operation.

As has been mentioned briefly above, before a customer is able to generate a postage mark they must first obtain postal credit from a recrediting centre (RC), and use this credit to charge their postal security device. Conveniently, obtaining credit from a recrediting centre and charging of PSDs can be accomplished on-line upon connection of the PSD to the RC. Once credit has been obtained the customer may then use their PSD (either as part of a PFM or a PC Franking system) to print digital postage marks onto envelopes or labels.

For security purposes, each PSD contains a number of cryptographic keys, some of which are unique to that PSD. In the preferred arrangement, each PSD contains a Main Franking Key, a Check Franking Key and an Integrity Key. The Main Franking Key and Check Franking Key are 16-byte triple-DES keys and The Integrity Key is a single-DES key. The PSD ensures that these keys are kept secret, and each PSD has a unique Main Franking Key

and Check Franking Key.

Single-DES block encryption is defined in the above mentioned standard FIPS46, and encryption of data in accordance with this standard under a key, k, is generally notated by $E_{DES}[k](data)$. Similarly, decryption of data under key k in accordance with this standard is notated by $D_{DES}[k](data)$. k and *data* each consist of eight bytes of information, each byte comprising eight bits with the most significant bit first. In this application it is assumed that the values of parity bits of a key (as defined in FIPS46) are ignored by the E_{DES} and D_{DES} functions.

Triple-DES block encryption has two forms which are concantenations (notated as "||") of 8 byte single-DES keys K_1, K_2 and K_3. The two forms of triple-DES encryption are a 16-byte key, $K = K_1 \| K_2$, and a 24-byte key $K = K_1 \| K_2 \| K_3$. As will later be described, these keys are used for different purposes in the system. Each of the two forms of encryption consist of alternating DES encryption and decryption.

The 16-byte Triple-DES form comprises the following functions:

$$E_{TDES2}[K](data) = E_{DES}[K_1](D_{DES}[K_2](E_{DES}[K_1](data)))$$

$$D_{TDES2}[K](data) = D_{DES}[K_1](E_{DES}[K_2](D_{DES}[K_1](data)))$$

The 24-byte Triple-DES form comprises the following functions:

$$E_{TDES3}[K](data) = E_{DES}[K_1](D_{DES}[K_2](E_{DES}[K_3](data)))$$

$$D_{TDES3}[K](data) = D_{DES}[K_1](E_{DES}[K_2](D_{DES}[K_3](data)))$$

Encryption of multiple blocks is accomplished with a form of Cipher

Block Chaining (CBC) as defined in the above mentioned FIPS81 standard. Using an encryption function in CBC mode reduces the possibility of attacks which generate valid messages by substituting encrypted blocks, and also forms the basis of a method for generating message authentication codes (MACs) (as will later be described).

To use the encryption function in CBC mode a sequence of n blocks of plaintext:

$$P = P_1 \| P_2 \| ... \| P_n$$

is transformed to blocks of ciphertext

$$C = C_1 \| C_2 \| ... \| C_n$$

where (using the notation "⊕" for exclusive OR):

$$C_1 = E_{TDES2}[K](P_1)$$

$$C_{i+1} = E_{TDES2}[K](C_i \oplus P_{i+1}) \text{ for } 1 \leq i < n$$

This process is illustrated schematically in Figure 11.

It will be understood from the above, and from Figure 11, that C_n is the notation for the value of the last enciphered block in a sequence, P, of n 8-byte blocks. The notation $E_{TDES2MAC}$ is also used, and is defined as follows:

$$E_{TDES2MAC}[K](P) = C_n$$

These keys are used to generate the aforementioned digital signature which is used to validate the DPM. For example, it is proposed that The Main Franking Key will be used as a normal check for use wherever DPMs are validated, and that The Check Franking Key will be used to determine

whether or not a Main Franking Key has been compromised. It is proposed that The Integrity Key will be used to provide basic confidentiality of, for example, the device reference (e.g. the identification number of the PSD) and item number, and also to provide a basic integrity check.

As is mentioned above, the Main Franking Key and Check Franking Key are unique to the PSD that holds them. The Integrity Key, is, in principle, common to all PSDs, but in practice it is likely that PSDs may be collected into sets and that each set will have a unique key.

The Main Franking Key and Check Franking Key are derived for each PSD from master keys, the Main Franking Master Key and Check Franking Master Key which are each 24-byte Triple-DES keys. The Main Franking Key and Check Franking Key are derived from these master keys.

The main and check franking keys are derived from their master keys by means of a hash function, MD5, defined in the RFC1321 standard mentioned above. Hash functions in general take a variable length input and generate a normally smaller output. In this context, the hash function would be described as being "one way". In the present case, the hash function takes an input, *data*, of arbitrary length and generates, in a relatively computationally-inexpensive process, two 64 bit halves of a 128 bit data block, represented as

$$\mathrm{MD5}(data) = \mathrm{Hash1} \,||\, \mathrm{Hash2}$$

In the present system, as will later be described, the *data* on which the

MD5 function operates is key data comprising a key version concantenated with a device reference (e.g. a PSD id).

The main franking key, and check franking key are generated as follows:

Main Franking Key = E_{TDES3}[Main Franking Master Key] (Hash1) || E_{TDES3}[Main Franking Master Key] (Hash2)

Check Franking Key = E_{TDES3}[Check Franking Master Key] (Hash1) || E_{TDES3}[Check Franking Master Key] (Hash2)

This process is illustrated schematically in Figure 12.

The appropriate authorities must protect these master keys. The authority holding the Check Franking Master Key in the preferred arrangement is separate from the authority holding the Main Franking Master Key. Master cryptographic keys are generated and, where necessary, distributed from the Key Distribution Centre (KDC). As mentioned above, PSDs are recredited by communicating with recrediting centres, which in the preferred arrangement are also responsible for distributing key updates to PSDs when necessary.

As is mentioned above, the DPM includes a MAC (message authentication code) data element encoded in the data matrix. The MAC is also used in the generation of the user-readable encrypted mark.

The MAC is constructed from other fields in the DPM, the Main Franking Key and the Check Franking Key and consists of two 20-bit fields:

The Main MAC, and The Check MAC. An Integrity Hash is appended to the MAC data field and is used as a low level, revenue protection check on the indicia.

The Integrity Hash is used to check on a DPMs integrity without risk of compromising the PSDs' Main Franking Keys or Check Franking Keys. The integrity protection, however, is not as strong as that provided by the MAC option. The Integrity hash is calculated using

Integrity Hash = first14bits (SHA-1 (Key Version || PSD Id || Item Data))

where "first14bits" means the bits in the 14 most significant bit positions in the result.

Data elements used for constructing the Integrity Hash, Main MAC and Check MAC are shown schematically in Figure 13.

As shown, in Figure 13, the Input Data consists of:

Input Data = Key Data || Item Data

The Key Data is used to identify the Main Franking Key and Check Franking Key, and consists of:

Key Data = Key Versions || PSD Id

where the PSD Id equals the device reference number concantenated with the device model number.

The Item Data consists of:

Item Data = Item Number || Date || Value || Service || Postcode

and the length of the Item Data in the preferred arrangement is equal to 216 bits. If the length of elements within the Item Data changes, then padding data (Pad1) is added to make the length of Item Data a multiple of 64 bits. It will be apparent, therefore, that in the present example Pad1 is 40 bits, to take to length of the item data to 256 bits.

The Main MAC comprises:

Main MAC = first20bits ($E_{TDES2MAC}$[Main Franking Key] (Item Data || Pad1))

where "firstnbits" means the bits in the "n" most significant bit positions in the result.

The Check MAC comprises:

Check MAC = first20bits($E_{TDES2MAC}$[Check Franking Key] (Item Data || Pad1))

The MAC generation process is summarised in Figure 14.

As mentioned above, it is possible that the data matrix used to encode the information may fail to be read – for example because it has been badly printed. To account for this possibility, encrypted user readable text is printed in the DPM so that assurance can be given that the indicia is legitimate even though the data matrix cannot be decoded.

The user readable text is encrypted using a derived integrity key, which changes on a daily basis, represented by:

Derived Integrity Key = E_{TDES2}[Integrity Key] (Date || Pad2)

where Pad2 is padding comprising 4 bytes of binary zeros.

Encrypted Data for the encrypted user readable mark is derived from the derived integrity key in accordance with the following function:

Encrypted Data = E_{TDES2}[Derived Integrity Key] (PSD id || User Readable Item Number || account reference)

The output of this encrypted data function is then converted to a 16 character hexadecimal number, where the first hexadecimal character represents the first 4 bits of the result, i.e. the first 4 most significant bit positions in the result. This hexadecimal number is then printed on the envelope as the aforementioned encrypted user readable mark.

It can be seen from the above that the integrity of the information encoded within the data matrix can be preserved by appending the MACs and/or (preferably "and") a digital signature derived from the above mentioned keys to the information. As a further advantage of this arrangement, integrity can still be preserved by means of the encrypted mark, even if the data matrix should be unreadable.

Post office facilities receiving postal items bearing DPMs can decode (or decrypt in the case of the encrypted user readable mark) the digital postage marks to reveal encrypted MACs and digital signatures, which can then be decrypted to allow the post office to validate the origin of the DPM.

The DPM, as will now be described, can also be used as part of a sophisticated revenue protection process that enables the post office to detect

attempted fraud. This particular invention is concerned with those persons who attempt to defraud the Post Office by using the same DPM on more than one postal item.

Figure 15 is a schematic representation of an integrated mail processor 150 which includes, in addition to the components of existing IMPs such as the one depicted in Figure 3 (which are referenced with the same numerals used in Figure 3), a DPM scanning station 152 and a revenue protection facility 154.

As postal items pass the DPM scanning station 152 of the IMP 150 the digital postage mark is scanned, and an image of the data matrix is captured by a logic device 156 connected to the scanning station and forming part of the revenue protection facility 154. The logic device 156 decodes the data matrix of the DPM to reveal the various data elements mentioned above which are encoded therewithin. If an image of the data matrix cannot be retrieved then, in this particular arrangement, the postal item concerned is rejected from the IMP for manual processing (as described in Figures 1 to 3).

Associated with the logic device 156 is a database 158 which stores data associated with one or more of the data elements encodable within a DPM. The information stored in the database, in the preferred arrangement, comprises information derived from postal items and associated DPMs that have already been processed by the IMP 150.

Once a given DPM has been scanned by the scanning station 158 and

the DPM has been decoded, the logic device 156 looks for data elements identifying the entity by whom the postal item in question has been sent.

The logic device then retrieves stored information for that entity from the database 158, and compares the stored information for that entity with information that has been decoded from the scanned data matrix for one or more corresponding data elements.

In this arrangement the database 158 stores a unique identifier, made up of the batch number and the item number (as described above), for each item of mail sent by a given entity (as identified by the account reference, the batch number and the data format identifier). Other arrangements will later be described.

In this arrangement the logic device 156 then looks for matches between the stored information and the scanned information, and if the logic device 156 should find a match between the information stored for that entity in the database and the corresponding information decoded from the data matrix, a flag is set identifying that a postal item with that unique identifier may have already been processed by the IMP.

Once the flag has been set the associated postal item is diverted to a store 160 for postal items with potentially fraudulent DPMs. Once in the store the DPM can be rechecked against the information stored in the database and further action can be taken if the match is confirmed.

If the logic device should determine that the decoded information is

different from that stored, then the DPM is determined to be valid and the postal item is allowed to continue to be processed in the manner described above in relation to Figure 3. The database is then updated to include the new postal item identifier decoded from the data matrix.

This revenue protection process is illustrated schematically as a flow diagram in Figure 16. In a first stage 160 the scanning station 152 attempts to scan a DPM from a postal item. In the next stage 162 the logic device 156 determines whether or not the data matrix has been adequately scanned. If the data matrix is unreadable then the postal item in question is rejected in step 164 from the IMP.

If the data matrix can be read, the logic device 156 - in step 166 - decodes information relating to data elements encoded within the data matrix (in this case information identifying the sending entity, and a unique identifier for that item of post). Next, in step 168, the logic device 156 retrieves stored data from the database 158, and in a next step 169, compares the retrieved stored data with the scanned data.

Then, in step 170, the logic device determines whether or not the scanned information matches the stored information. If the logic device should detect a match in step 170, then the item of post concerned is diverted from the IMP to a store for postal items with potentially fraudulent DPMs where the item can be rechecked. If no match is detected then processing of the item is allowed to continue, in step 172, and the database is updated in

step 174 to include the postal item identifier decoded from the data matrix.

It can be seen therefore that this arrangement provides the Post Office with an effective means to detect attempted fraud.

In the preferred arrangement this process is accomplished in real time, with the data matrix being decoded and the check against the database being made within a very short time of the data matrix being scanned.

However, as this arrangement requires the database to be continuously updated with postal item identifiers to generate a list of postal item identifiers for each entity it is possible, and probably likely, that the database would very quickly become too large to enable the checks to be made before the postal item moves to the next processing stage in the IMP. To help alleviate this problem, one could move the step at which mail is rejected further down the chain of functions performed by the IMP, for example to just before the postal items are sorted by the sorter 65 (Figure 3) to provide more time for the database to be interrogated and the checks to be made.

In an alternative arrangement, which also alleviates this drawback, the database can be arranged to store only a running total for each sending entity so that it does not need to store a separate data item for the sending entities each time a DPM is scanned.

As mentioned above, each PSD needs to be charged with postal credit before the PSD can be used to generate DPMs. As a result, the Post Office know how much credit has been stored on each PSD.

This total credit information can be stored in the database for each sending entity, and can then be debited on a continuous basis with the postal value data element decoded from the data matrix (or indeed the user readable postal value printed outside the data matrix on the envelope) to provide a real time indication of the postal credit stored on the PSD. The postal credit information stored in the database can be updated each time postal credit is purchased for a given PSD.

If the logic device should detect a postal value in a DPM where the database indicates that the entity concerned has insufficient postal credit (for example zero (or less) postal credit) stored on their PSD, then the logic device can operate to divert the postal item concerned on the basis that the postal value which is purported to have been debited from the PSD (by virtue of it appearing on a DPM) cannot actually have been debited as the PSD would not appear to have contained sufficient credit to permit the DPM to be generated.

This arrangement avoids the minor drawbacks associated with the first arrangement since it would only be necessary to store a single value, which is continuously updated, for each entity in the database.

The principles of this arrangement may be adapted as required for the sensing of other data elements of the DPM. For example, as described above the data matrix includes an item identifier which is continuously incremented as DPMs are generated by PSDs. This item identifier is also printed on the front of the postal item as a user readable indication.

As a result, the post office know that scanned item identifiers should in general increase as DPMs are generated until the identifier assumes the ASCII value 999999, whereupon it resets to 000000 and starts increasing once more.

If the database is arranged to include a current item identifier for each entity (the current item identifier being the maximum identifier that has previously been scanned), then the Post Office can use this information to determine whether or not a given DPM is likely to be valid. For example, if the database indicates that the maximum item identifier for a given entity is currently stored as 123456, for example, then a DPM with an item identifier of 101235 is likely to be fraudulent as one would expect the item identifier to be larger than that currently stored (as the item identifier is incremented by 1 each time a DPM is generated). Such an item could then be diverted from the IMP for manual checking.

It will be apparent to persons skilled in the art that for this arrangement to work in practise it will be necessary to set a threshold for the minimum item identifier that will be accepted as valid as it cannot be guaranteed that postal items will be processed by the IMP in the order that the DPMs are generated by the PSD. This threshold could be varied in accordance with information identifying the sending entity to take account of how trustworthy a given sending entity has been in the past.

For example, for those entities who have previously not attempted to

defraud the post office the minimum acceptable item identifier could be set to be significantly lower than the maximum identifier previously stored (for example 25% lower). For less trustworthy entities the minimum acceptable identifier could be much larger than this, for example only 5% lower.

The database could be arranged to store both the maximum identifier previously scanned and the minimum acceptable identifier, or more preferably the database could be arranged to store only the minimum acceptable identifier. In either case the database would be updated whenever a new identifier is read that has a value greater than that previously stored.

If the user readable representation of the item identifier is read from the DPM, as opposed to the item identifier encoded within the data matrix, then the above described process can be simplified as it is then no longer necessary to decode the data matrix.

The principle of identifying untrustworthy sending entities could also be expanded so that all postal items emanating from a given entity are flagged as being "suspicious", and are diverted for detailed checking.

It will be apparent from the above that many alternative arrangements may be employed to check for fraudulent behaviour. For example the Post Office may maintain records indicating the likely number of postal items that will be sent by a given entity on a daily basis so that mail can be diverted for checking if the number of items sent should suddenly increase (as might happen if one batch were held back so that previously used DPMs could be

copied onto the items). As a result, the present description should not be read as limiting the invention in any way.

In a further alternative to the first arrangement, the user readable encrypted mark could be read as an alternative, or in addition to, reading the data matrix as the user readable encrypted mark will be unique for each DPM.

In general terms, the present invention should be understood to relate to a method where information is read from a DPM (n.b. that information does not necessarily have to be coded or encrypted information), and the read information is compared to stored information to determine the validity of the read DPM; and also to apparatus operable to accomplish that method.

It will also be understood, and should be noted, that the particular embodiments described herein are provided only by way of example. Persons skilled in the art will no doubt be capable of devising modifications and alterations to the embodiments described which whilst being different to the modifications and alterations mentioned will nevertheless still be within the scope of the present invention as defined in the accompanying claims.

For example, whilst in figure 15 the revenue protection facility and DPM scanner are shown as being part of an IMP it will be apparent that they could instead be provided in a stand-alone machine through which postal items are fed either before or after they are fed through the IMP. They could also be incorporated in any of a number of alternative machines or processes. For example, the scanner could comprise a hand scanner operated by persons

working in a dedicated revenue protection facility or indeed in any one of the other facilities illustrated in Figures 1 or 2.

CLAIMS

1. A method of authenticating a postage mark comprising the steps of:

extracting an item of information from one component of the mark,

extracting a corresponding item of information from a database;

comparing the items of information extracted from the postage mark and the database, and

determining the validity of the postage mark on the basis of said comparison.

2. A method according to Claim 1 wherein the item of information is encoded in said component of the mark.

3. A method according to Claim 2, wherein the information item is encoded within a data matrix.

4. A method according to Claim 1, 2 or 3, wherein the item of information is encrypted in said component of the mark.

5. A method according to any preceding claim, wherein the item of information is represented as plain text (i.e. user readable) in said component of the mark.

6. A method according to any preceding claim, wherein the corresponding item of information stored in the database comprises an item of information that has previously been extracted from a postage mark.

7. A method according to any preceding claim, comprising adding, if the postage mark is determined to be valid, the information item extracted from the postage mark to the database of information items.

8. A method according to any preceding claim, wherein the item of information of the postage mark comprises a unique identifier for the postal item associated with the postage mark.

9. A method according to Claim 8, wherein the postal item unique identifier comprises a batch number and an item number.

10. A method according to claim 8 or 9, wherein:

the database stores sending entity information and associated extracted items of information, and

wherein the method comprises:

extracting sending entity information from the postage mark and comparing an information item extracted from the postage mark with the information items stored in said database for the entity identified by said

entity sending information.

11. A method according to any of claims 6 to 10, wherein the postage mark is determined to be valid if the extracted information item is different from the corresponding information item stored in the database.

12. A method according to any of claims 6 to 11, wherein the postage mark is determined to be invalid if the extracted information item is the same as the corresponding information item stored in the database.

13. A method according to any of claims 1 to 7, wherein: the information item extracted from the postage mark comprises an item identifier; the database stores a highest previously extracted item identifier; and wherein in said determining step the mark is determined to be valid if said extracted item identifier is greater than the stored item identifier.

14. A method according to Claim 13, wherein said mark is also determined to be valid if said item identifier is within a predetermined range below said item identifier.

15. A method according to Claim 13 or 14 comprising replacing the stored item identifier in the database with the extracted item identifier if said

extracted identifier is determined to be greater than said stored item identifier.

16. A method according to any of claims 1 to 7, wherein: the information item extracted from the postage mark comprises an item identifier; the database stores an item identifier comprising a minimum item identifier of a predetermined range of identifiers below a maximum previously extracted item identifier; and wherein in said determining step the mark is determined to be valid if said extracted item identifier is greater than the stored minimum item identifier.

17. A method according to Claim 16 comprising replacing the stored item identifier in the database with the extracted item identifier if said extracted identifier is determined to be greater than said stored item identifier.

18. A method according to any of claims 1 to 7, wherein: the information item extracted from the postage mark comprises a postage price identifier; the database stores an indication of postage credit purchased by an entity; and wherein in said determining step the mark is determined to be valid if the credit indication is sufficient to enable the postage price indicated by said identifier to be debited therefrom.

19. A method substantially as hereinbefore described.

20. A computer program product comprising one or more software portion which when executed in an execution environment are configured to perform one or more of the method steps of any Claims 1 to 19.

21. An envelope with a postage mark printed thereon, the mark comprising one or more information items represented as intelligible user readable text, and one or more information items encoded within a data matrix and/or encrypted within a user readable (but unintelligible) mark.

22. Apparatus for authenticating a postage mark comprising:

means for extracting an item of information from one component of the mark,

means for extracting a corresponding item of information from a database;

means for comparing the items of information extracted from the postage mark and the database, and

means for determining the validity of the postage mark on the basis of said comparison.

23. Apparatus for authenticating a postage mark substantially as hereinbefore described with reference to the accompanying drawings.

24. An integrated mail processor comprising apparatus according to Claim 22 or 23.

25. An integrated mail processor substantially as hereinbefore described with reference to the accompanying drawings.

26. A method of generating a postage mark suitable for use in the method of any of Claims 1 to 19, the method comprising the steps of providing a plain text (i.e. user readable) representation of a plurality of information items in one component of said postage mark, and encoding or encrypting a plurality of information items in another component of the postage mark.

27. A method according to Claim 26, wherein at least one information item is included in each component of said postage mark.

The Patent Office
PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
INVESTOR IN PEOPLE

Application No: GB 0106663.8
Claims searched: 1 to 19, 22 to 25

Examiner: John Donaldson
Date of search: 4 October 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4M(MCA)

Int Cl (Ed.7): G06K 5/00, 7/00, 7/10, 7/12, 7/14, 17/00

Other: Online:WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X, E	WO 02/50765 A1	(PITNEY BOWES), see abstract, column 10, lines 7 to 25	1 to 6, 8 to 10, 22, 24
X	WO 00/31692 A1	(PTT POST), see abstract, page 29, line 33 to page 32, line 8	1 to 10, 18, 22, 24
X	US 6039257	(BERSON), see abstract, column 4, line 57 to column 5, line 13	1 to 6, 8 to 10, 22, 24
X	US 5929415	(BERSON), see abstract, column 5, lines 1 to 31	1 to 6, 8 to 10, 22, 24
X	US 5917925	(MOORE), see abstract, column 4, lines 26 to 46	1 to 6, 8 to 10, 22, 24
X	US 5801364	(KARA), see abstract	1 to 6, 8 to 10, 22, 24

X Document indicating lack of novelty or inventive step
Y Document indicating lack of inventive step if combined with one or more other documents of same category.
& Member of the same patent family
A Document indicating technological background and/or state of the art.
P Document published on or after the declared priority date but before the filing date of this invention.
E Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB_____2376332A_I_>